FIM - Windows & Linux File Integrity Monitoring

Name: Sameer Hassan
SOC ANALYST

Lab # 02

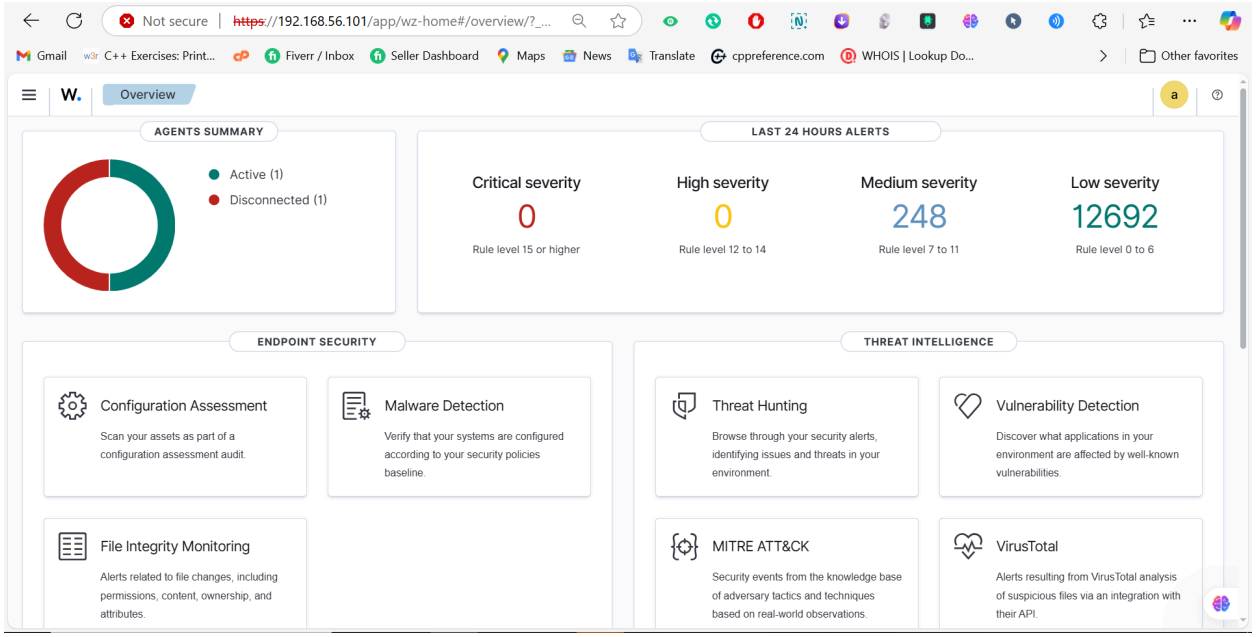
What's FIM?

File Integrity Monitoring (FIM) is a security process that checks and alerts you when your system files are altered, added, or deleted. It helps detect unauthorized changes and ensures the integrity and security of your data.

FIM

- File Integrity Monitoring (FIM) is a security process.
- It checks and alerts you when files are altered, added, or deleted on your system.
- FIM helps detect unauthorized changes.
- It ensures the integrity and security of your data.

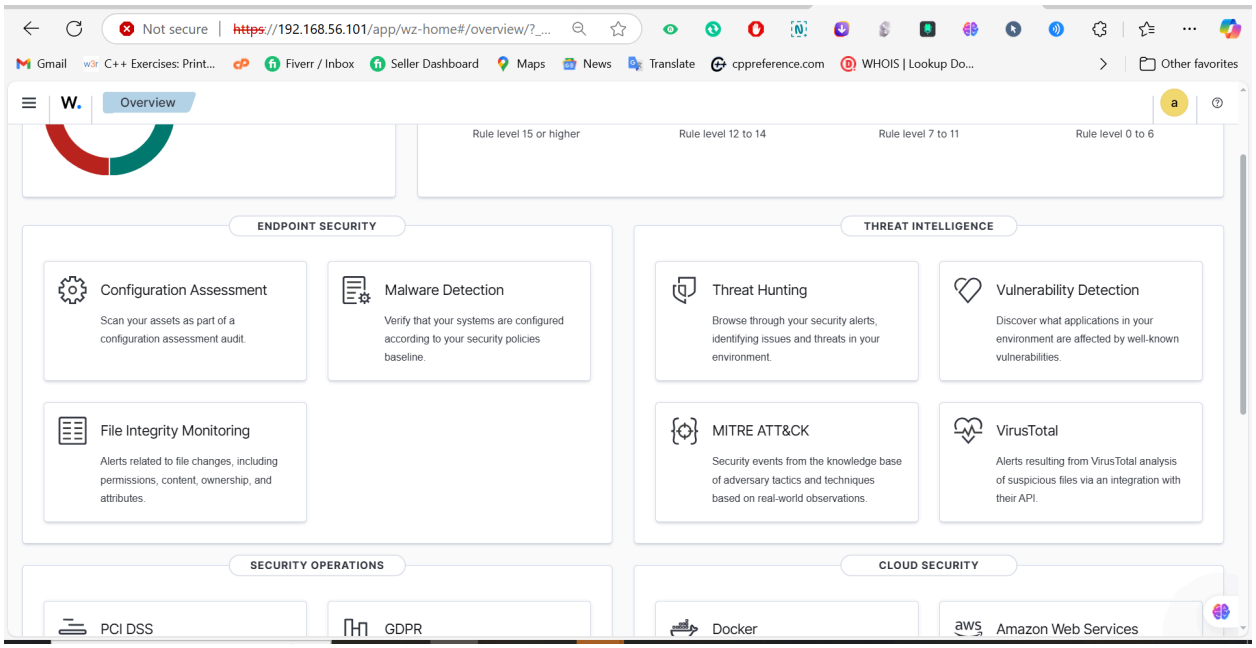
Open Your Wazuh dashboard

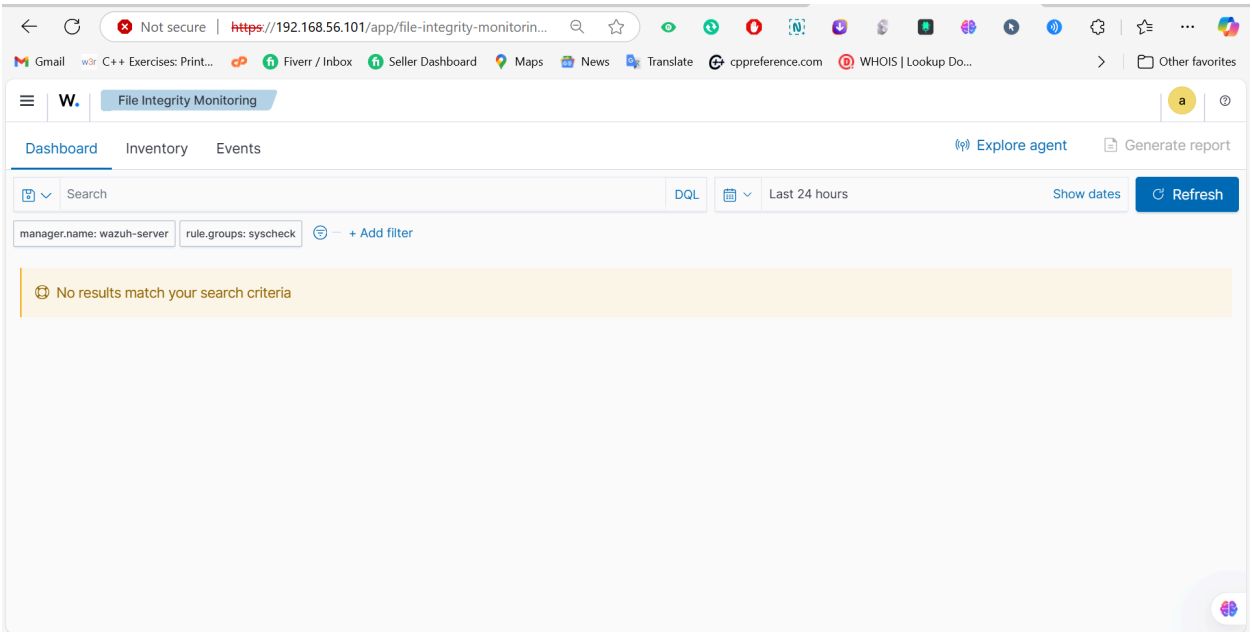


I have two Agents integrated with Wazuh 1 is active and 1 is deactivated/Offline.

CONFIGURING FIM

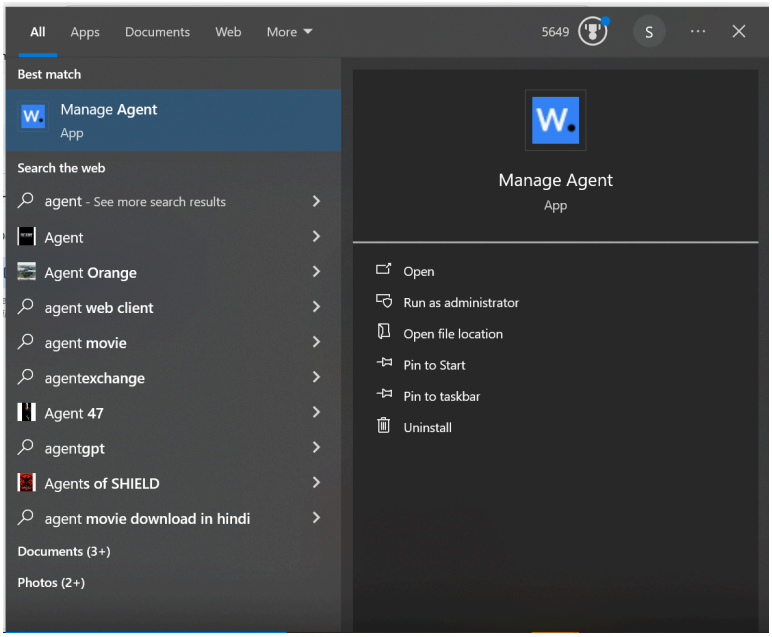
Under Endpoint Security we have a Option named File Integrity Monitoring click on it

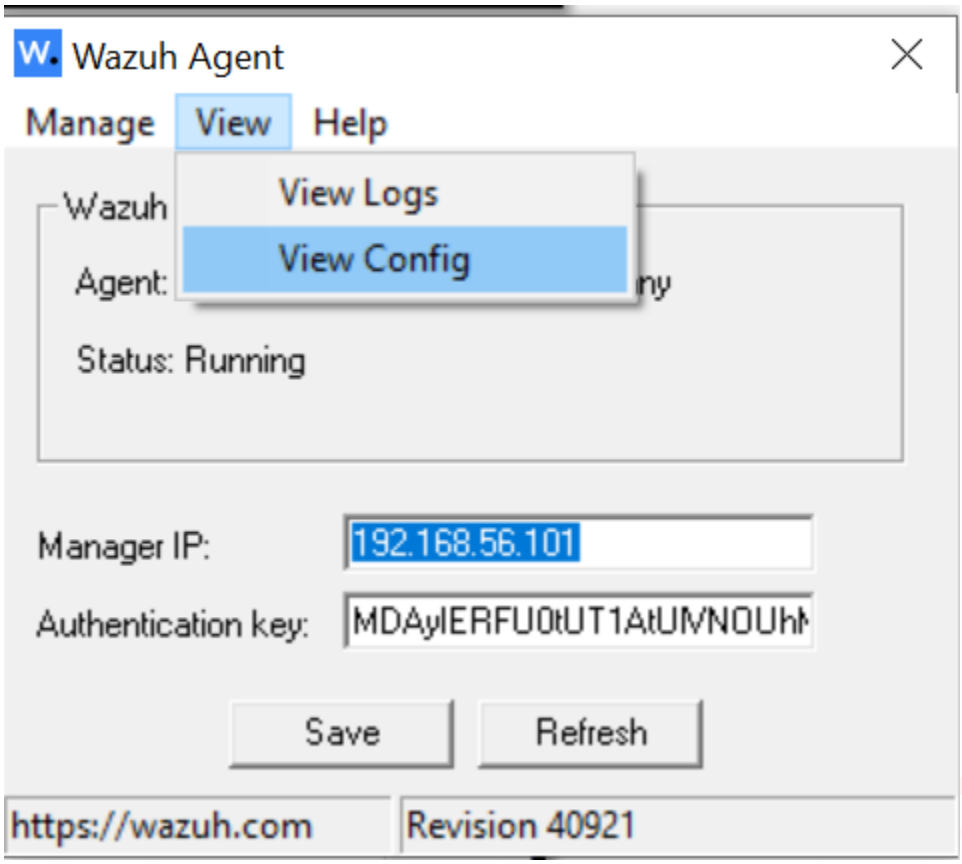




No data is showing.

To configure FIM open Agnet on your Windows OS as administrator.





Click on view then select view Config

It will directly open **OSSEC.CONF** file or you can simply open this file by visiting the OSSEC folder.

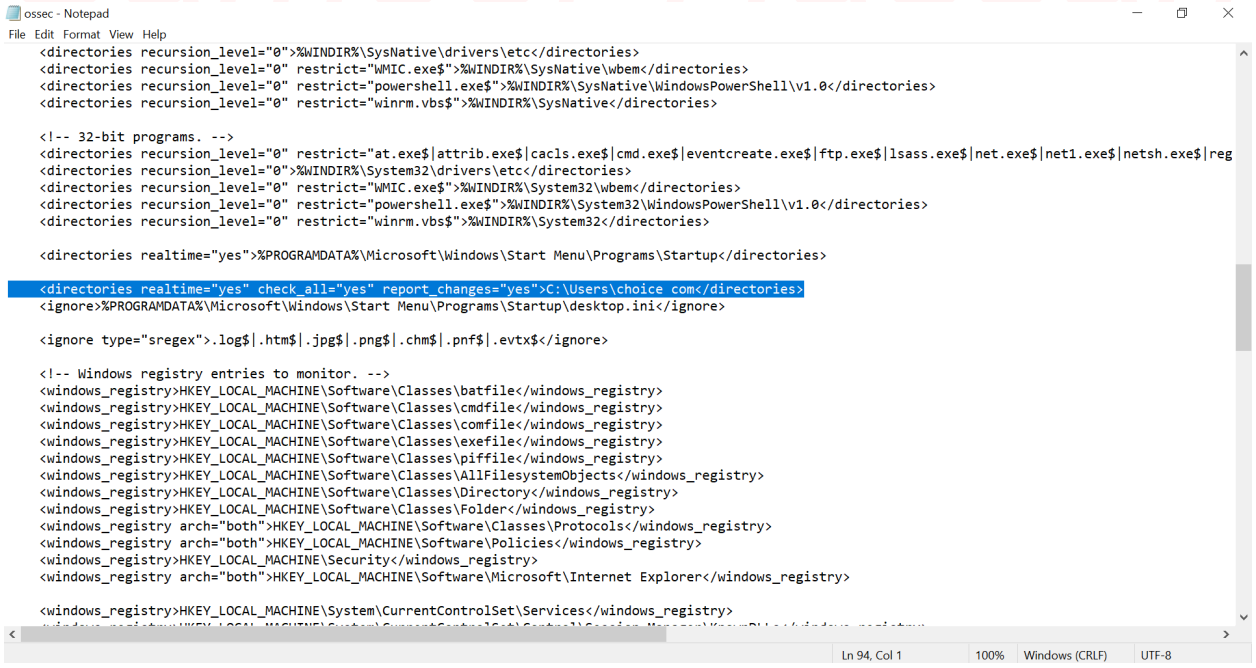
Scroll Down and you will found File Integrity Monitoring and Under this, you will find <syschk> Under this you will see so many Directories tags

<directories recursion_level="0"

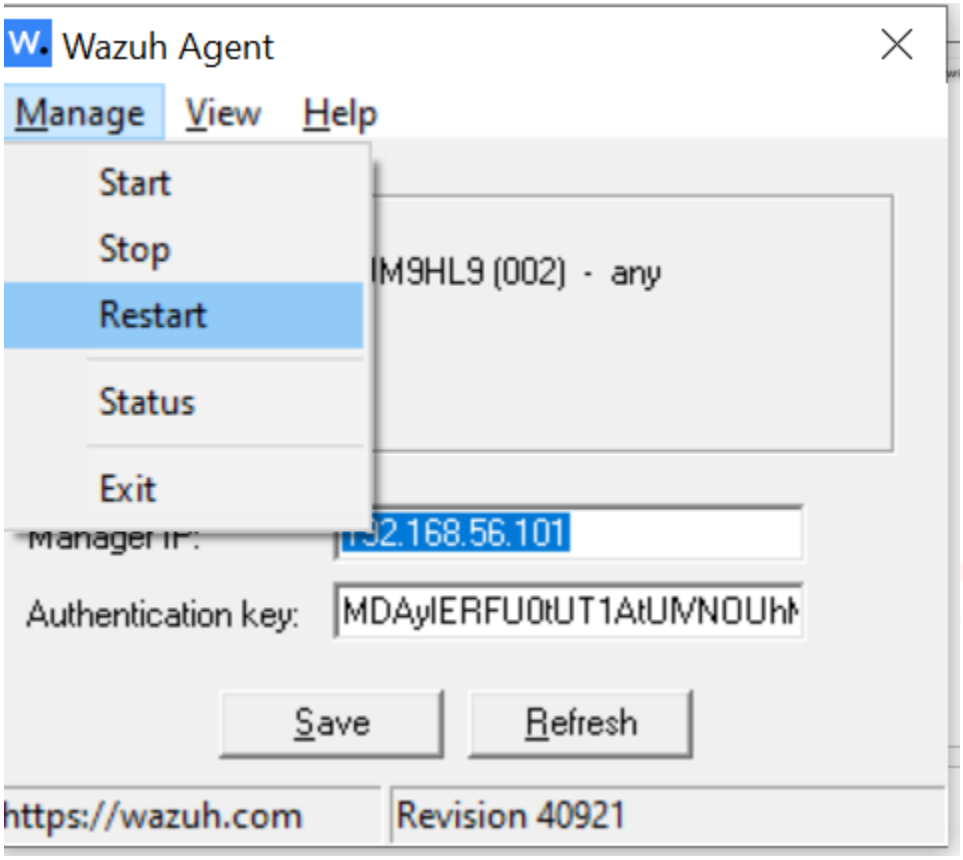
restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

Simply add the Folder or drive path you want to monitor.
To add you just replace C:\Users\choice com
<directories realtime="yes" check_all="yes" report_changes="yes">C:\Users\choice com</directories>

I added my Choice Com folder to monitor you can add any folder you want!!

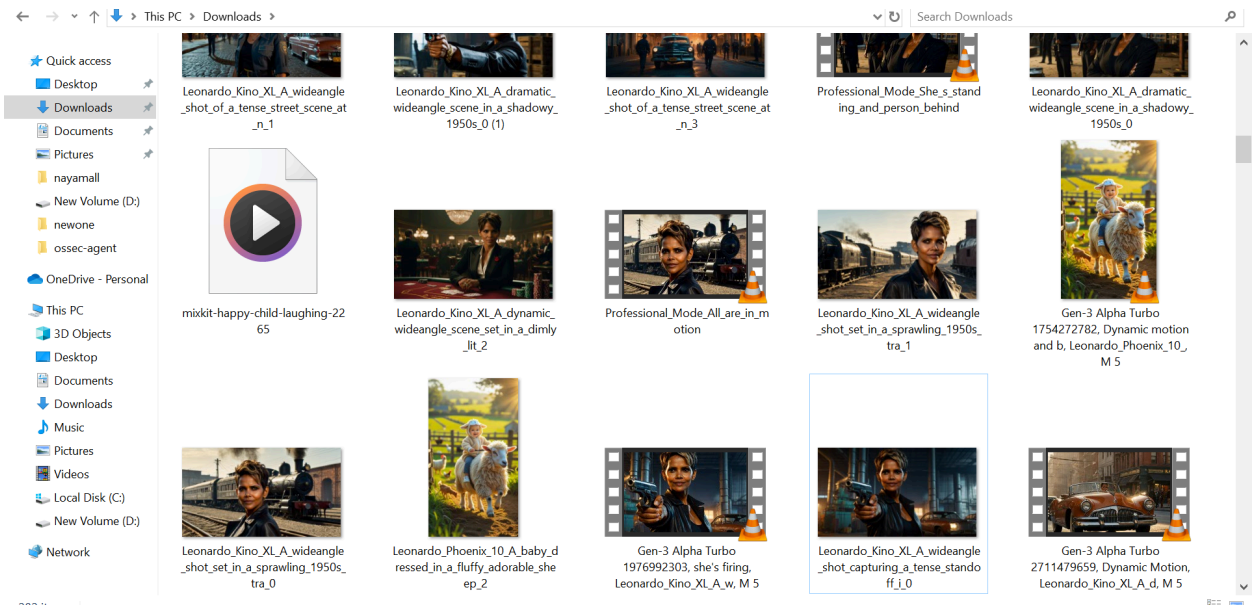


After writing this command save the file and Restart the agent!



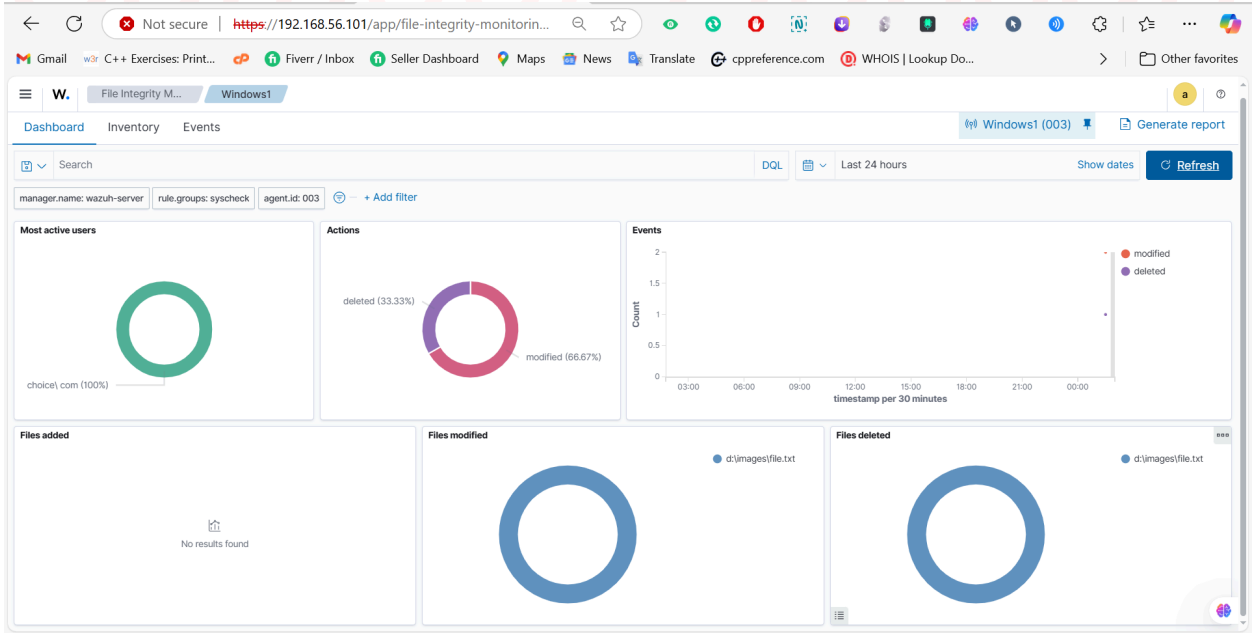
Testing the Configration

You can delete, Edit or remove any file from the folder you added and you will see the log in Wazuh



Perform any action on file you will see the result in Wazuh.

I deleted 2 files, let's check the Logs.

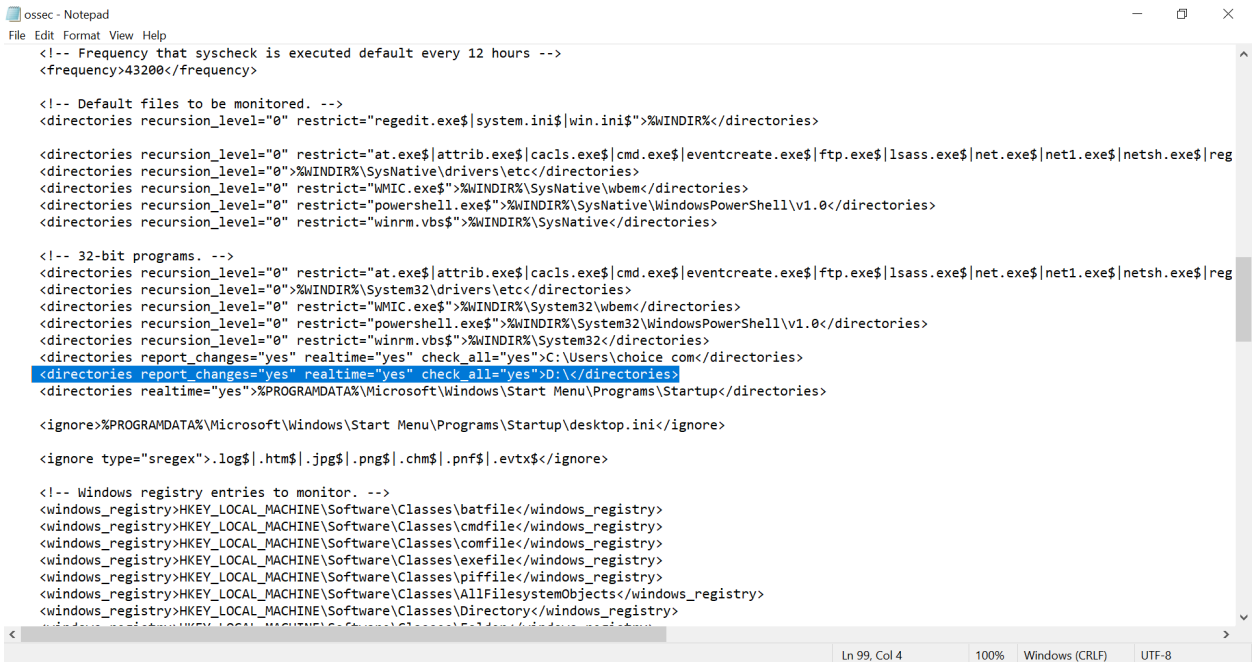


Successfully Configured!

Verification

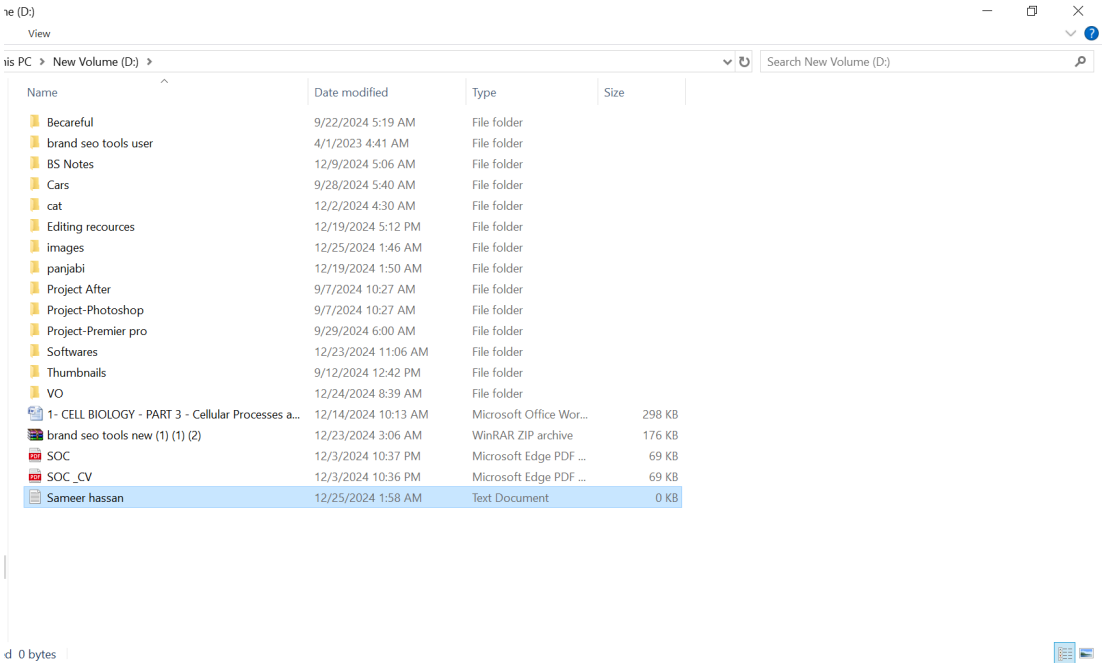
Add the path of any folder you want to monitor.

I added my D drive path.

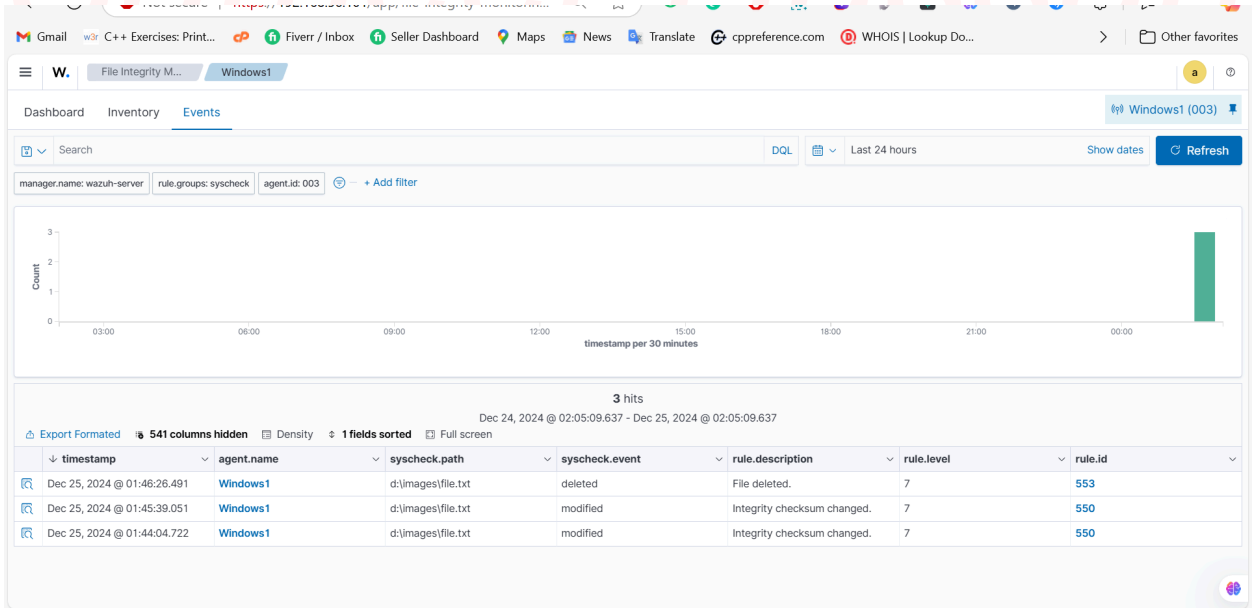


After adding the path restart the agent!

Now let's create a new file and add some text to it.

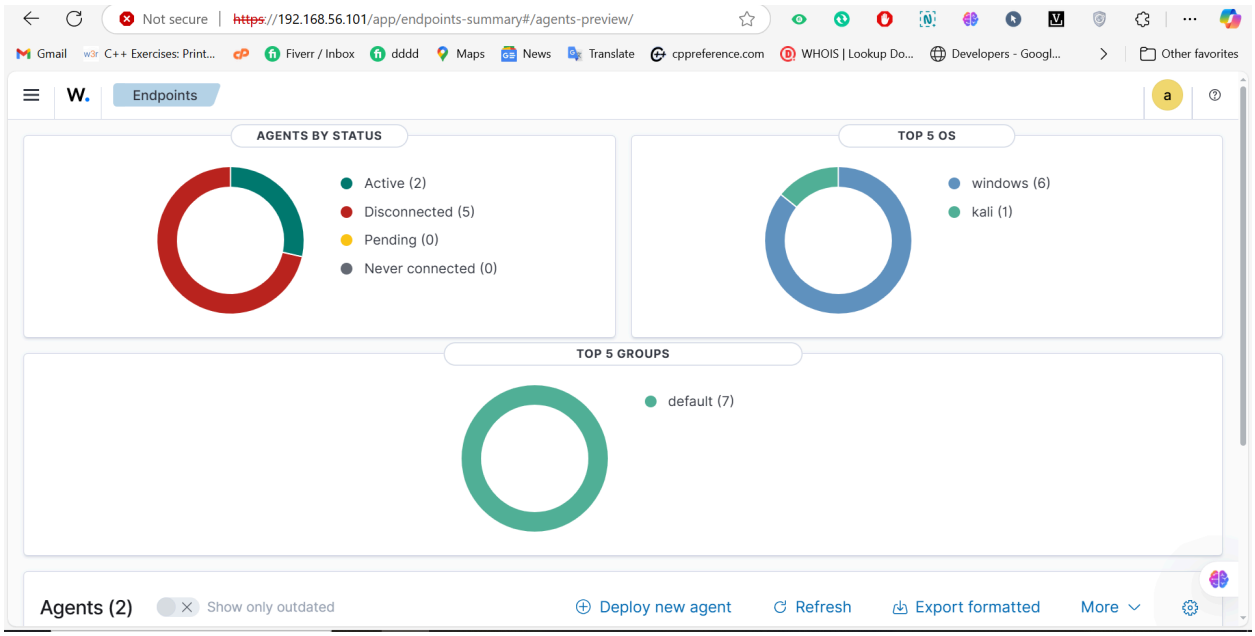


I created a new file named Sameer Hassan let check Wazuh to view the file D drive log.

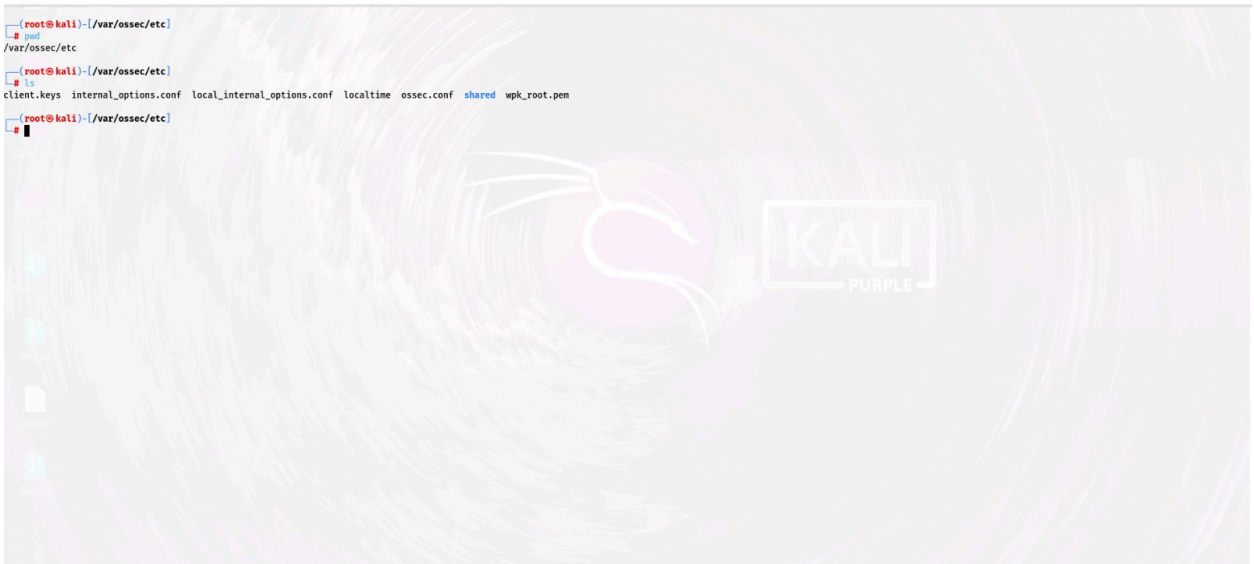


Windows FIM is Configured!

Now let's configure the Ubuntu Environment FIM.

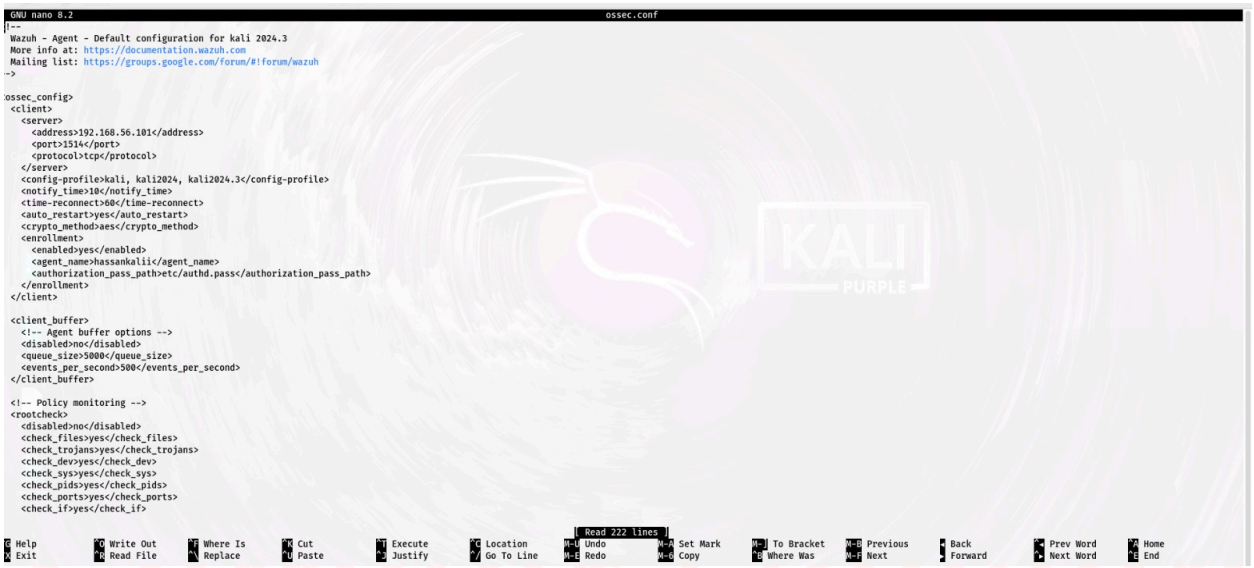


Two agents are active Windows and another is Ubuntu kali-linux.

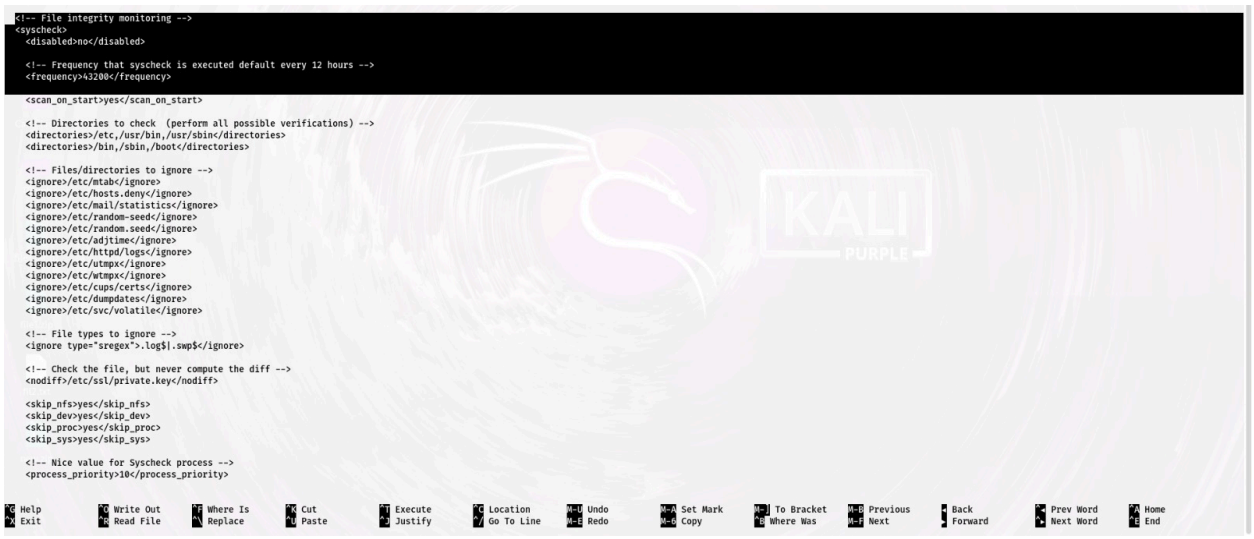


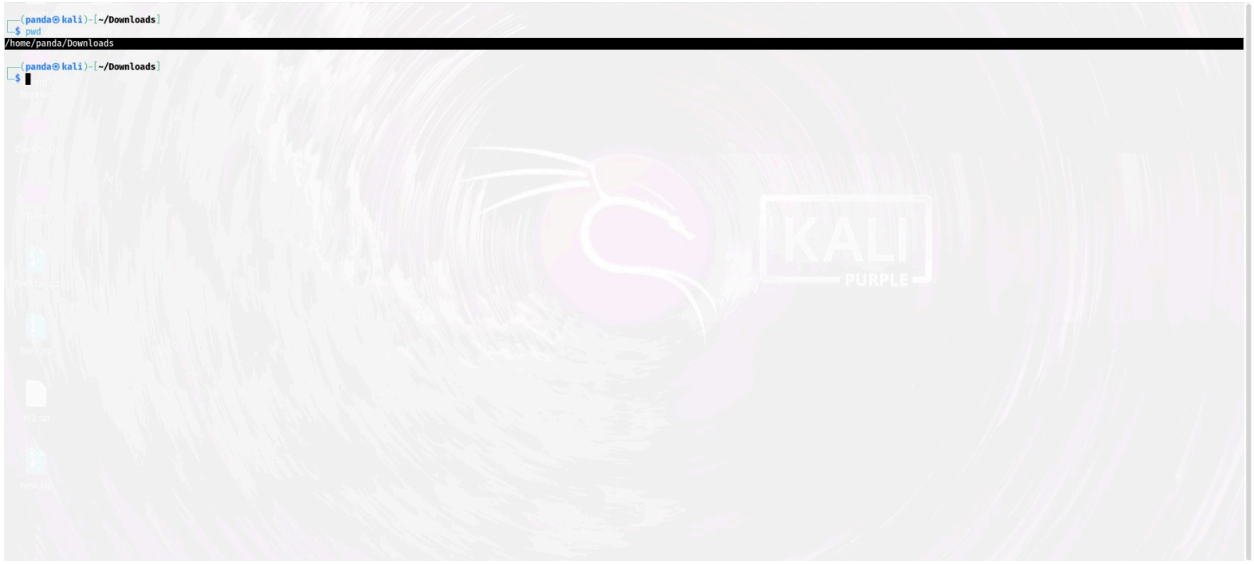
Visit directory /var/ossec/etc and there you will found OSSEC.conf file.

Open file uisng nano ossec.conf or gedit ossec.conf

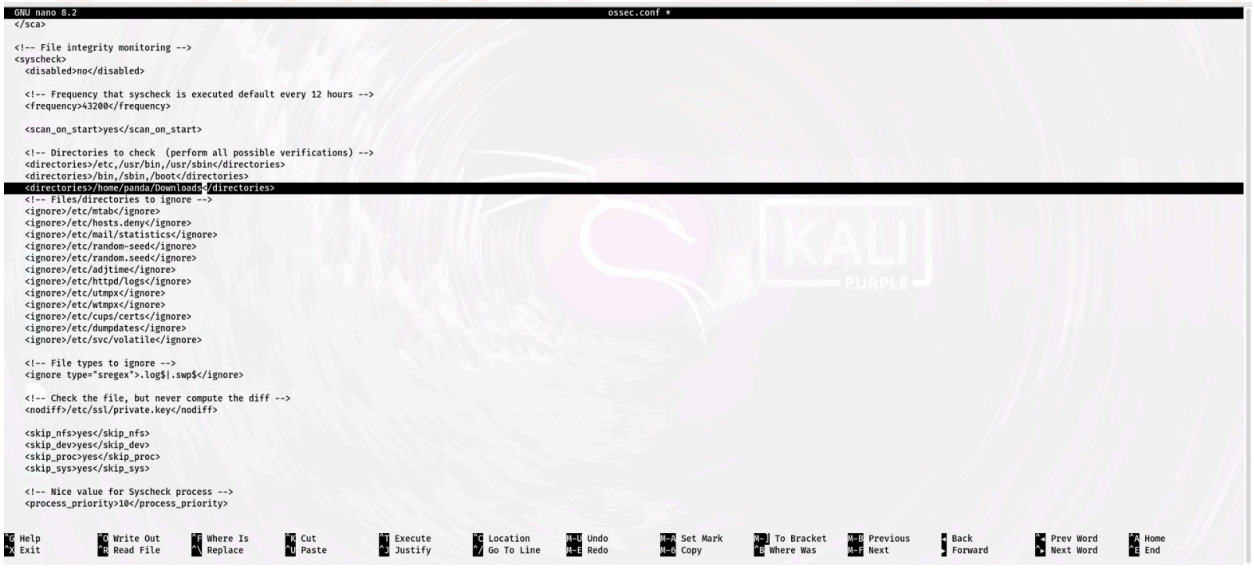


After opening the OSSEC.CONF file visit File Integrity Monitoring section as we did in the Windows FIM section.





Copy directory path you want to add in FIM
I copied my download path.



I added my Download directory path
You can add this using
<directories check_all="yes">/home/panda/Downloads</directories>

After adding the path save the file and restart the agent. Using command systemctl restart wazuh-agent

Summary

Wazuh's File Integrity Monitoring provides comprehensive monitoring capabilities, ensuring the security and integrity of your files. It tracks changes in real-time, detects unauthorized modifications, and offers detailed reports for enhanced protection against potential threats and data breaches.